FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005-3315

202 • 408 • 4000
FACSIMILE 202 • 408 • 4400

ATLANTA
404•653•6400
PALO ALTO
650•849•6600

WRITER'S DIRECT DIAL NUMBER:

(202) 408-4024

TOKYO
011•813•3431•6943
BRUSSELS
011•322•646•0353

March 3, 2000

ATTORNEY DOCKET NO.: 04329.2244

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

New U.S. Patent Application
Title: CRYPTOGRAPHIC COMMUNICATION TERMINAL, CRYPTOGRAPHIC COMMUNICATION CENTER APPARATUS, CRYPTOGRAPHIC COMMUNICATION SYSTEM, AND STORAGE MEDIUM

Inventors and Addresses:

Kouya TOCHIKUBO
Yokohama-shi, Japan

Naoki ENDOH
Fuchu-shi, Japan

Sir:

We enclose the following papers for filing in the United States Patent and Trademark Office in connection with the above patent application.

1. A check for $708 representing the filing fee.

2. Application - 47 pages, including 2 independent claims and 21 claims total.

3. Drawings - 6 sheets of formal drawings containing 7 figures.

4. Certified copy of Japanese Application No. 11-058592, filed March 5, 1999.

This application is being filed under the provisions of 37 C.F.R. § 1.53(f). Applicants await notification from the Patent and Trademark Office of the time set for filing the Declaration.

Applicants claim the right to priority based on Japanese Application No. 11-058592, filed March 5, 1999.

Please accord this application a serial number and filing date.

The Commissioner is hereby authorized to charge any additional filing fees due and any other fees due under 37 C.F.R. § 1.16 or § 1.17 during the pendency of this application to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By: _____
Richard V. Burgujian
Reg. No. 31,744

RVB/FPD/dvz
Enclosures

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ３月 ５日

出 願 番 号
Application Number: 平成１１年特許願第０５８５９２号

出 願 人
Applicant (s): 株式会社東芝

２０００年 １月２８日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３００１１６８

【書類名】　特許願

【整理番号】　A009900214

【提出日】　平成11年 3月 5日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

G06F 7/00

【発明の名称】　暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体

【請求項の数】　17

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　栃窪　孝也

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　遠藤　直樹

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体

【特許請求の範囲】

【請求項１】　暗号通信における情報送受信の一方となる暗号通信端末において、

前記暗号通信に用いる暗号アルゴリズムを１種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部と、

前記暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部と、

前記暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、前記暗号アルゴリズム格納部及び前記鍵情報格納部に対してそれぞれ指定する制御手段と、

前記暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び前記鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段と

を備えたことを特徴とする暗号通信端末。

【請求項２】　前記暗号アルゴリズム格納部は、暗号化された暗号アルゴリズムを格納するとともに、

前記暗号化された暗号アルゴリズムを復号化する暗号アルゴリズム復号化手段を備えたことを特徴とする請求項１記載の暗号通信端末。

【請求項３】　前記鍵情報格納部は、前記暗号通信用の鍵の他、暗号化された暗号アルゴリズムを復号化する際に用いるアルゴリズム復号化鍵を格納することを特徴とする請求項２記載の暗号通信端末。

【請求項４】　前記鍵情報格納部は、暗号化された鍵を格納するとともに、

前記暗号化された鍵を復号化する鍵情報復号化手段を備えたことを特徴とする請求項１乃至３のうち何れか一項に記載の暗号通信端末。

【請求項５】　前記制御手段は、前記暗号アルゴリズム格納部に格納する何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アル

ゴリズムを出力するよう前記暗号アルゴリズム格納部に指令し、

前記暗号化・復号化手段は、前記要求暗号アルゴリズムを前記送信する情報として暗号化することを特徴とする請求項１乃至４のうち何れか一項に記載の暗号通信端末。

【請求項６】　自己の通信相手が請求項５の暗号通信端末又は請求項１乃至６のうち何れか一項に記載の暗号通信端末を備える装置である場合に、当該通信相手に新たな暗号アルゴリズム及び又はこれに対応するアルゴリズム復号化鍵を要求し、その応答を暗号化・復号化手段にて復号化するとともに、

要求した暗号アルゴリズムを受け取った場合にはこれを前記暗号アルゴリズム格納部に格納し、要求したアルゴリズム復号鍵を受け取った場合にはこれを前記鍵情報格納部に格納することを特徴とする請求項１乃至５のうち何れか一項に記載の暗号通信端末。

【請求項７】　前記請求項１乃至６のうち何れか一項に記載の暗号通信端末を備えるとともに、

通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力することを特徴とする暗号通信センター装置。

【請求項８】　前記請求項５記載の暗号通信端末を備える場合に、

前記アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納する更新用暗号アルゴリズム格納部を備え、

前記制御手段は、前記暗号通信端末から暗号アルゴリズムを要求された場合には、前記暗号アルゴリズム格納部に代え、前記更新用暗号アルゴリズム格納部に対して前記要求暗号アルゴリズムを前記送信する情報として出力するよう指令することを特徴とする請求項７記載の暗号通信センター装置。

【請求項９】　前記暗号通信端末から前記アルゴリズム復号化鍵を要求された場合に、送信すべきアルゴリズム復号化鍵を暗号化し、この暗号化されたアルゴリズム復号化鍵を前記送信する情報として前記暗号化・復号化手段に入力する鍵暗号化手段を備えたことを特徴とする請求項７又は８記載の暗号通信センター装置。

【請求項１０】　前記鍵暗号化手段は、送信相手の暗号通信端末が固有に備える鍵により前記アルゴリズム復号化鍵を暗号化することを特徴とする請求項７乃至９のうち何れか一項に記載の暗号通信センター装置。

【請求項１１】　２以上の前記請求項１乃至６のうち何れか一項に記載の暗号通信端末が設けられた暗号通信システム。

【請求項１２】　１以上の前記請求項１乃至６のうち何れか一項に記載の暗号通信端末と前記請求項７乃至１０のうち何れか一項に記載の暗号通信センター装置とが設けられた暗号通信システム。

【請求項１３】　暗号通信における情報送受信の一方となる暗号通信装置に用いられるプログラムであって、

前記暗号通信に用いる暗号アルゴリズムを１種類以上格納させるとともに、指定された暗号アルゴリズムを出力させる暗号アルゴリズム格納手段と、

前記暗号アルゴリズムに対応した暗号通信用の鍵を格納させるとともに、指定された鍵を出力させる鍵情報格納手段と、

前記暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、前記暗号アルゴリズム格納手段及び前記鍵情報格納手段に対してそれぞれ指定させる制御手段と、

前記暗号アルゴリズム格納手段に対して指定された暗号アルゴリズム及び前記鍵情報格納手段に対して指定された鍵によって、受信した暗号情報を復号化させ、又は、送信する情報を暗号化させる暗号化・復号化手段と

を有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項１４】　前記暗号アルゴリズム格納手段は、暗号化された暗号アルゴリズムを格納させるとともに、

前記暗号化された暗号アルゴリズムを、アルゴリズム復号化鍵によって復号化させる暗号アルゴリズム復号化手段を有するプログラムを記憶した請求項１３記載の記憶媒体。

【請求項１５】　前記制御手段は、前記暗号アルゴリズム格納手段に格納させる何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アルゴリズムを出力させるよう前記暗号アルゴリズム格納手段に指令させ、

前記暗号化・復号化手段は、前記要求暗号アルゴリズムを前記送信する情報として暗号化させるプログラムを記憶した請求項１３又は１４記載の記憶媒体。

【請求項１６】　通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力させることプログラムを記憶した請求項１４又は１５記載の記憶媒体。

【請求項１７】　前記アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納させる更新用暗号アルゴリズム格納手段と、

通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力させる手段とを有し、

前記制御手段は、前記暗号通信端末から暗号アルゴリズムを要求された場合には、前記更新用暗号アルゴリズム格納手段に対して要求暗号アルゴリズムを前記送信する情報として出力させるよう指令させるプログラムを記憶した請求項１４記載の暗号通信センター装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体、更に詳しくは複数の暗号アルゴリズムが使用可能であり、かつ新規暗号アルゴリズムを安全かつ効率よく登録し使用可能である部分に特徴のある暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体に関する。

【０００２】

【従来の技術】

現在、ネットワークに接続された種々の機器には機密保持のために暗号化技術が組み込まれている。この組み込まれた暗号化技術を用いることで、ネットワークを介する電子商取引やコンテンツ配信事業等が盛んに行われようとしている。それらの業務は組み込まれている暗号化技術の安全性のもとに成り立っているものであり、このような背景から安全かつ効率の良い暗号アルゴリズムの設計に関

する研究が盛んに行われている。

【０００３】

しかしながら、暗号化技術を組み込んだ従来のシステムでは、規格標準化等によりシステム仕様が一度決まってしまうと、それと同時に、システムで使用する暗号方式が固定されてしまう。したがって、システムのセキュリティレベルも固定されることになる。

【０００４】

一方、安全な暗号アルゴリズムの設計に関する研究と同時に暗号アルゴリズムの安全性の評価のために暗号アルゴリズムの解読法の研究も盛んに行われている。したがって、システムで使用している暗号方式が解読されるといったことも現実に起こりうることである。

【０００５】

このようにシステムで使用している暗号方式が破られてしまった場合には、暗号方式を更新しない限り、当該システムをそのまま使用することができなくなる。すなわち安全なネットワーク通信を継続するには、システムの暗号方式を更新する必要が生じる。

【０００６】

【発明が解決しようとする課題】

しかしながら、ネットワークを介しての暗号方式更新は、秘密情報の外部への流出等の安全性の面で問題がある。一方、ネットワークを介さない変更では、システムのすべての機器に一台づつに暗号方式変更を加えなければならず、効率的な変更が不可能である。

【０００７】

本発明は、このような実情を考慮してなされたもので、その第１の目的は、暗号アルゴリズムを選択的して暗号通信を行うことができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することにある。

【０００８】

また、第２の目的は、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる暗

号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することにある。

【０００９】

【課題を解決するための手段】

上記課題を解決するために、請求項１に対応する発明は、暗号通信における情報送受信の一方となる暗号通信端末において、暗号通信に用いる暗号アルゴリズムを１種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部と、暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部と、暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、暗号アルゴリズム格納部及び鍵情報格納部に対してそれぞれ指定する制御手段と、暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段とを備えた暗号通信端末である。

【００１０】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的して暗号通信を行うことができる。これにより、より安全な暗号方式を選択して暗号通信を行うことができる。

【００１１】

次に、請求項２に対応する発明は、請求項１に対応する発明において、暗号アルゴリズム格納部は、暗号化された暗号アルゴリズムを格納するとともに、暗号化された暗号アルゴリズムを復号化する暗号アルゴリズム復号化手段を備えた暗号通信端末である。

【００１２】

本発明はこのような手段を設けたので、端末装置において暗号アルゴリズムの安全性を確保することができ、ひいては暗号通信の秘匿性を高めることができる。

【００１３】

次に、請求項３に対応する発明は、請求項２に対応する発明において、鍵情報

格納部は、暗号通信用の鍵の他、暗号化された暗号アルゴリズムを復号化する際に用いるアルゴリズム復号化鍵を格納する暗号通信端末である。

【００１４】

本発明はこのような手段を設けたので、請求項２に対応する発明と同様に暗号アルゴリズムを第三者から守ることができる。

【００１５】

次に、請求項４に対応する発明は、請求項１～３に対応する発明において、鍵情報格納部は、暗号化された鍵を格納するとともに、暗号化された鍵を復号化する鍵情報復号化手段を備えた暗号通信端末である。

【００１６】

本発明はこのような手段を設けたので、暗号通信用の鍵やアルゴリズム復号化鍵を安全な状態で保持することができ、第三者に鍵を盗まれた場合でも、暗号アルゴリズム自体や通信鍵の安全性を確保することができ、ひいては暗号通信の秘匿性を高めることができる。

【００１７】

次に、請求項５に対応する発明は、請求項１～４に対応する発明において、制御手段は、暗号アルゴリズム格納部に格納する何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アルゴリズムを出力するよう暗号アルゴリズム格納部に指令し、暗号化・復号化手段は、要求暗号アルゴリズムを送信する情報として暗号化する暗号通信端末である。

【００１８】

本発明はこのような手段を設けたので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録することができる。

【００１９】

次に、請求項６に対応する発明は、請求項１～５に対応する発明において、自己の通信相手が請求項５の暗号通信端末又は請求項１乃至６のうち何れか一項に記載の暗号通信端末を備える装置である場合に、当該通信相手に新たな暗号アルゴリズム及び又はこれに対応するアルゴリズム復号化鍵を要求し、その応答を暗号化・復号化手段にて復号化するとともに、要求した暗号アルゴリズムを受け取

った場合にはこれを暗号アルゴリズム格納部に格納し、要求したアルゴリズム復号鍵を受け取った場合にはこれを前記鍵情報格納部に格納する暗号通信端末である。

【００２０】

本発明はこのような手段を設けたので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる。

【００２１】

次に、請求項７に対応する発明は、請求項１乃至６のうち何れか一項に記載の暗号通信端末を備えるとともに、通信相手からアルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への送信する情報として暗号化・復号化手段に入力する暗号通信センター装置である。

【００２２】

本発明はこのような手段を設けたので、アルゴリズム復号化鍵を集中的に管理し、端末からアルゴリズム復号化鍵の要求があったときにはこれを暗号通信でもって引き渡すことができる。

【００２３】

次に、請求項８に対応する発明は、請求項７に対応する発明において、請求項５記載の暗号通信端末を備える場合に、アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納する更新用暗号アルゴリズム格納部を備え、制御手段は、暗号通信端末から暗号アルゴリズムを要求された場合には、暗号アルゴリズム格納部に代え、更新用暗号アルゴリズム格納部に対して要求暗号アルゴリズムを送信する情報として出力するよう指令する暗号通信センター装置である。

【００２４】

本発明はこのような手段を設けたので、アルゴリズム復号鍵のみならず、暗号アルゴリズム自体も安全に要求端末に送信することができる。

【００２５】

次に、請求項９に対応する発明は、請求項７又は８に対応する発明において、

暗号通信端末からアルゴリズム復号化鍵を要求された場合に、送信すべきアルゴリズム復号化鍵を暗号化し、この暗号化されたアルゴリズム復号化鍵を送信する情報として暗号化・復号化手段に入力する鍵暗号化手段を備えた暗号通信センター装置である。

【００２６】

本発明はこのような手段を設けたので、暗号通信における暗号化に加えて元々の鍵自体も暗号化されるのでより安全にアルゴリズム復号化鍵を引き渡すことができる。

【００２７】

次に、請求項１０に対応する発明は、請求項７～９に対応する発明において、鍵暗号化手段は、送信相手の暗号通信端末が固有に備える鍵によりアルゴリズム復号化鍵を暗号化する暗号通信センター装置である。

【００２８】

本発明はこのような手段を設けたので、要求を発した端末のみに対応する形でアルゴリズム復号化鍵を暗号化でき、安全性をより一層高めることができる。

【００２９】

次に、請求項１１に対応する発明は、２以上の前記請求項１乃至６のうち何れか一項に記載の暗号通信端末が設けられた暗号通信システムである。

【００３０】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的して暗号通信を行うことができる暗号通信システムを構築することができる。

【００３１】

次に、請求項１２に対応する発明は、１以上の請求項１乃至６のうち何れか一項に記載の暗号通信端末と請求項７乃至１０のうち何れか一項に記載の暗号通信センター装置とが設けられた暗号通信システムである。

【００３２】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的して暗号通信を行うことができるとともに、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることが

できる暗号通信システムを構築することができる。

【００３３】

次に、請求項１３に対応する発明は、請求項１に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００３４】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項１の暗号通信端末として機能する。

【００３５】

次に、請求項１４に対応する発明は、請求項２に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００３６】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２の暗号通信端末として機能する。

【００３７】

次に、請求項１５に対応する発明は、請求項５に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００３８】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項５の暗号通信端末として機能する。

【００３９】

次に、請求項１６に対応する発明は、請求項７に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００４０】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項７の暗号通信センター装置として機能する。

【００４１】

次に、請求項１７に対応する発明は、請求項８に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【００４２】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項８の暗号通信センター装置として機能する。

【００４３】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【００４４】

なお、各実施形態では、暗号化されたデータをＥ１（ｘ）［ｙ］、Ｅ２（ｘ）［ｙ］、Ｅ（ｚ，ｘ）［ｙ］等と表す。ここで、ｘは暗号化に用いる鍵を表し、ｙは暗号化対象のデータを表し、ｚは暗号化に用いるアルゴリズムを表す。また、ａ｜ｂはａとｂの連接を表す。

【００４５】

（発明の第１の実施の形態）

図１は本発明の第１の実施の形態に係る暗号通信システムの一例を示す構成図である。

【００４６】

同図に示す暗号通信システムは、インターネットやＬＡＮ等の種々のネットワーク１に暗号通信端末２（以下、単に端末２ともいう）及び暗号通信センター装置３（以下、単にセンター３ともいう）が接続されて構成されている。各端末２間、及び端末２～センター３間ではネットワーク１を介して通信（あるいは暗号通信）が実行可能に構成されている。

【００４７】

図２は暗号通信端末の構成例を示すブロック図である。

【００４８】

暗号通信端末２は、制御部１１、鍵情報格納部１２、暗号アルゴリズム格納部１３、暗号化・復号化部１４、鍵情報復号化部１５、暗号アルゴリズム復号化部１６及びＩＤ格納部１７から構成されている。この端末２は、ＣＰＵやメモリ等の計算機要素を備えた手段であり、プログラムに制御されるＣＰＵの動作により上記各機能手段を実現している。また、ネットワーク通信のために、図示しない通信装置を備えている。

【００４９】

一方、図３は暗号通信センター装置の構成例を示すブロック図である。

【００５０】

暗号通信センター装置３は、制御部２１、鍵情報格納部２２、暗号アルゴリズム格納部２３、暗号化・復号化部２４、端末鍵情報格納部２５、アルゴリズム復号化鍵格納部２６、鍵暗号化部２７、更新用暗号アルゴリズム格納部２８、端末権限管理部２９及びＩＤ格納部３０から構成されている。センター３は、端末２と同様、ＣＰＵやメモリ等の計算機要素を備えた手段であり、プログラムに制御されるＣＰＵの動作により上記各機能手段を実現している。また、ネットワーク通信のために、図示しない通信装置を備えている。

【００５１】

ここでまず、暗号通信端末２の各構成要素について説明する。

【００５２】

制御部１１は、各部１２～１７を制御することでデータの流れを制御し、例えば識別情報（ＩＤ）やメッセージ等を機能部１２，１３，１４に与える。また、制御部１１は、ＩＤ情報を指定することで暗号通信の際に使用する秘密鍵や暗号アルゴリズムを選択するようになっている。

【００５３】

ＩＤ格納部１７は、センター３及び端末２のＩＤや、アルゴリズム（Ａ１）のＩＤ、更には鍵のＩＤ等、種々のＩＤを格納する。

【００５４】

鍵情報格納部１２は、暗号化された鍵情報を格納しており、端末等のＩＤ及びアルゴリズムＩＤを入力されると、これらに対応しかつ暗号化された鍵情報を鍵情報復号化部１５に出力する。

【００５５】

鍵情報復号化部１５は、鍵情報格納部１２から引き渡された鍵情報を自己の固有の秘密鍵で復号化し出力する。

【００５６】

暗号アルゴリズム格納部１３は、暗号化されたアルゴリズムを格納しており、

アルゴリズムＩＤを入力されると、これに対応しかつ暗号化された暗号アルゴリズムを暗号アルゴリズム復号化部１６に出力する。

【００５７】

暗号アルゴリズム復号化部１６は、鍵情報復号化部１５から受け取った鍵を用いて暗号アルゴリズム格納部１３から出力された暗号アルゴリズムを復号する。

【００５８】

暗号化・復号化部１４は、暗号アルゴリズム復号化部１６により復号されたアルゴリズムを用い、鍵情報復号化部１５にて復号化された通信用の鍵によってメッセージMを暗号化する。

【００５９】

次に、暗号通信センター装置の各構成要素について説明する。

【００６０】

制御部２１は、各部２２～３０の動作を制御して情報の流れを制御するとともに、ＩＤ等を対応する機能部に与える。また、制御部１２は、ＩＤ情報を指定することで暗号通信の際に使用する秘密鍵や暗号アルゴリズムを選択するとともに、端末２が更新要求する暗号アルゴリズムやその復号化鍵を選択するようになっている。

【００６１】

鍵情報格納部２２は、各端末２とセンター３間で暗号通信するための秘密鍵を格納するとともに、端末ＩＤを受け取ると対応する秘密鍵を暗号化・復号化部２４に出力する。

【００６２】

暗号アルゴリズム格納部２３は、種々の暗号アルゴリズムを格納しており、アルゴリズムＩＤを受け取ると、対応する暗号アルゴリズムを暗号化・復号化部２４に出力する。

【００６３】

端末鍵情報格納部２５は、各端末の固有の秘密鍵を格納しており、端末ＩＤを受け取ると、対応する端末の秘密鍵を鍵暗号化部２７に出力する。

【００６４】

アルゴリズム復号化鍵格納部２６は、暗号化された各暗号アルゴリズムの復号化鍵を格納しており、アルゴリズムＩＤを受け取ると、対応する暗号アルゴリズムの復号化鍵を鍵暗号化部２７に出力する。

【００６５】

鍵暗号化部２７は、端末固有の秘密鍵によって暗号アルゴリズムの復号化鍵を暗号化し暗号化・復号化部２４に出力する。

【００６６】

更新用暗号アルゴリズム格納部２８は、端末２に与えるべき新たな暗号アルゴリズムを格納しており、アルゴリズムＩＤを受け取ると、これに対応しかつ暗号化された暗号アルゴリズムを暗号化・復号化部２４に出力する。

【００６７】

暗号化・復号化部２４は、鍵暗号化部２７から出力されたアルゴリズム復号化鍵及び又は更新用暗号アルゴリズム格納部２８から出力された暗号アルゴリズムを、暗号アルゴリズム格納部２３からの暗号アルゴリズムを用い、鍵情報格納部２２から受け取った鍵により暗号化する。

【００６８】

端末権限管理部２９は、更新用暗号アルゴリズムやそのアルゴリズム復号化鍵を要求する端末が正当権限を有するものであるかをチェックし、正当権限を揺する場合のみ、上記各部２１～２８による処理を許可する。

【００６９】

ＩＤ格納部３０は、端末や、アルゴリズム、アルゴリズム復号鍵等のＩＤを格納しており、何れかの端末２からＩＤ取得要求があったときには、そのＩＤを要求端末２に送信する。

【００７０】

次に、以上のように構成された本実施形態における暗号通信システムの動作について説明する。

【００７１】

まず、端末間暗号通信について説明する。

【００７２】

図４は端末間で暗号通信が行われる様子を示す図である。

【００７３】

同図では、端末２ｉから端末２ｊへメッセージMが暗号アルゴリズムＡ１で暗号化されて送信される手順が示されている。

【００７４】

この場合まず、送信先の端末２ｊの名前やメールアドレス等のＩＤ情報ＩＤｊと暗号通信の際使用する暗号アルゴリズムＡ１のＩＤ情報ＩＤＡ１とが端末２ｉの制御部１１によってＩＤ格納部１７から取り出される。また、メッセージMが制御部１１に入力される。すなわち制御部１１は使用する暗号アルゴリズムの指定手段としても機能している。なお、端末２ｉ及び２ｊは、予め必要なＩＤ情報をセンター３に請求し、当該センター３におけるＩＤ格納部３０のＩＤ情報を取得している。

【００７５】

メッセージMは制御部１１から暗号化・復号化部１４に出力される。同様に、ＩＤＡ１は暗号アルゴリズム格納部に出力され、ＩＤｊ及びＩＤＡ１が鍵情報格納部１２に出力される。

【００７６】

ここで、鍵情報格納部１２においては入力されたＩＤ情報より、対応する鍵情報が取り出され、鍵情報復号化部１５に出力される。すなわちＩＤｊにより暗号化された秘密鍵Ｅ１（Ｋｉ）［Ｋｉｊ］が出力され、ＩＤＡ１によりアルゴリズム復号化鍵Ｅ１（Ｋｉ）［ＫＡ１］が出力される。ここで、Ｋｉｊは端末２ｉ，２ｊ間で暗号通信を行うための鍵であって、例えばＤＥＳの共通鍵等が相当する。

【００７７】

この暗号化された鍵情報は、鍵情報復号化部１５においてパスワードやＩＣカードに保存されている鍵などの端末固有の鍵情報Ｋｉによって復号化される。このうち、暗号化されたアルゴリズムＡ１の復号化鍵であるＫＡ１は暗号アルゴリズム復号化部１６へ、Ｋｉｊは暗号化・復号化部１４へそれぞれ出力される。

【００７８】

一方、暗号アルゴリズム格納部１６からは、制御部１１から入力されたＩＤ情報に基づいて暗号アルゴリズム復号化部１６に対し暗号化された暗号アルゴリズムＥ２（ＫＡｌ）［Ａｌ］が出力される。

【００７９】

この入力された暗号化された暗号アルゴリズムは、暗号アルゴリズム復号化部１６においてアルゴリズム復号化鍵ＫＡｌによって復号化され、暗号化・復号化部１４に対して暗号化アルゴリズムＡｌとして出力される。

【００８０】

暗号化・復号化部１４においては、入力されたメッセージM、暗号アルゴリズムＡｌ、秘密鍵Ｋｉｊによって送信するメッセージMが暗号化される。

【００８１】

こうして作成された暗号文Ｅ（Ａｌ，Ｋｉｊ）［M］には、送信元端末を示すＩＤｉと、この暗号通信で使用する暗号アルゴリズムのＩＤＡｌが添付され、図示しない送信装置によりネットワーク１を介して端末２ｊに送信される。

【００８２】

この暗号通信を受け取った端末２ｊにおいては、まず、制御部１１からＩＤＡｌが暗号アルゴリズム格納部１３に出力され、ＩＤｉ及びＩＤＡｌが鍵情報格納部１２に出力される。

【００８３】

このＩＤ情報が入力された情報格納部１２より、鍵情報復号化部１５に対して暗号化された秘密鍵Ｅｌ（Ｋｊ）［Ｋｉｊ］及びアルゴリズム復号化鍵Ｅｌ（Ｋｊ）［ＫＡｌ］が出力される。

【００８４】

暗号化されたこれらの鍵情報はパスワードやＩＣカードに保存されている鍵などの端末固有の鍵情報Ｋｊによって鍵情報復号化部１５において復号化され、このうちＫＡｌは暗号アルゴリズム復号化部１６へ、またＫｉｊは暗号化・復号化部１４へそれぞれ出力される。

【００８５】

一方、制御部１１から暗号アルゴリズム格納部１３に入力されたＩＤ情報に基

づき、当該暗号アルゴリズム格納部１３から暗号アルゴリズム復号化部１６に対して暗号化された暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］が出力される。

【００８６】

暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］は、暗号アルゴリズム復号化部１６においてアルゴリズム復号化鍵ＫＡ１により復号化され、暗号化・復号化部に対しアルゴリズムＡ１として出力される。

【００８７】

暗号化・復号化部１４においては、端末２ｉから受け取った暗号文Ｅ（Ａ１，Ｋｉｊ）［M］が暗号アルゴリズムＡ１及び秘密鍵Ｋｉｊによって復号化され、メッセージMが出力される。

【００８８】

このようにして、端末２ｉから端末２ｊへの暗号アルゴリズムＡ１による暗号通信が実現されることになる。このとき、最初に与えるアルゴリズムＩＤは適宜変更可能であるので、端末２ｉ，２ｊの双方が登録している暗号アルゴリズムであればこれを自在に変更できる。

【００８９】

次に、端末２が保持していない暗号アルゴリズムをセンター３から取得し、新たな暗号アルゴリズムを登録する登録（更新）手順について説明する。この更新手続きには暗号通信センター装置３から暗号アルゴリズム及びその復号鍵のすべてを取得する更新手順＃１と、暗号アルゴリズムは他の暗号通信端末２から取得し、その復号鍵はセンター３から取得する更新手順＃２とがある。ここでは、更新手順＃１を説明し、第２の実施形態で更新手順＃２を説明する。

【００９０】

図５は暗号アルゴリズム及びその復号鍵のすべてを暗号通信センター装置３から取得する更新手順＃１の処理を示す図である。

【００９１】

同図では端末２ｉがセンターに対し、新しい暗号アルゴリズムＡ１′及び暗号アルゴリズムＡ１′に対する暗号アルゴリズム復号化鍵ＫＡ１′を要求する場合を示している。

【００９２】

このためにまず、端末２ｉからセンター３に、端末２ｉのＩＤ情報ＩＤｉ、更新する暗号アルゴリズムのＩＤ情報ＩＤＡ１′、更新の際使用する暗号アルゴリズムのＩＤ情報ＩＤＡ１が送信される。なお、ＩＤ情報ＩＤＡ１′等は事前に端末２ｉにおいてセンター３から取得され、ＩＤ格納部１７に格納されている。

【００９３】

各ＩＤ情報を受け取った暗号通信センター装置３においては、受信情報が制御部２１に読み込まれる。さらに、制御部２１から端末権限管理部２９への問合せが行われて端末２ｉが暗号アルゴリズムを取得する権限を備えているかが確認される。必要な場合には、端末２ｉは自己を証明する暗証情報等を送信し、その暗証情報等が端末権限管理部２９での権限確認に用いられる。なお、権限確認された後に、制御部２１への読み込みが行われてもよい。

【００９４】

権限確認後、制御部２１にて読み込まれた各ＩＤについて、当該制御部２１から暗号アルゴリズム格納部２３に対してＩＤＡ１が出力され、また、鍵情報格納部２２に対しＩＤｉが出力される。さらに、端末鍵情報格納部２５に対しＩＤｉが出力され、アルゴリズム復号化鍵格納部２６に対しＩＤＡ１′が出力され、更新用暗号アルゴリズム格納部２８に対しＩＤＡ１′が出力される。

【００９５】

この制御部２１からのＩＤ情報出力に対応し、まず、暗号アルゴリズム格納部２３からは暗号化・復号化部２４に対し暗号アルゴリズムＡ１が出力される。また、鍵情報格納部２２からは暗号化・復号化部２４に対し鍵Ｋｃｉが出力される。ここで、鍵Ｋｃｉは、端末２ｉとセンター３間で暗号通信を行うための共通秘密鍵（例えばＤＥＳ用の鍵）である。

【００９６】

さらに、入力されたＩＤ情報各々に対応し、端末鍵情報格納部２５からは鍵暗号化部２７に対して端末２ｉ固有の鍵Ｋｉが出力され、アルゴリズム復号化鍵格納部２６からは鍵暗号化部２７に対しアルゴリズムＫＡ１′用の鍵ＫＡ１′が出力される。なお、暗号通信センター装置３は、端末権限管理部２９に登録された

すべての暗号通信端末２の固有の鍵（Ｋｉ，Ｋｊ等）を保持している。

【００９７】

鍵暗号化部２７においては、入力された端末２ｉ固有の鍵Ｋｉとアルゴリズム復号化鍵ＫＡ１′よって、鍵ＫＡ１′が鍵Ｋｉで暗号化され、その暗号化結果としてＥ１（Ｋｉ）［ＫＡ１′］が暗号化・復号化部２４に出力される。

【００９８】

一方、入力されたＩＤ情報に基づき、更新用暗号アルゴリズム格納部２８から暗号化・復号化部２４に対しＥ２（ＫＡ１′）［Ａ１′］が出力される。なお、Ｅ２（ＫＡ１′）［Ａ１′］は、端末２ｉから要求された暗号アルゴリズムＡ１′が鍵ＫＡ１′によって暗号化されたものである。

【００９９】

こうして暗号化・復号化部２４に対しては、暗号アルゴリズムＡ１、秘密鍵Ｋｃｉ、更新情報Ｅ１（Ｋｉ）［ＫＡ１′］及びＥ２（ＫＡ１′）［Ａ１′］が入力される。更新情報Ｅ１（Ｋｉ）［ＫＡ１′］及びＥ２（ＫＡ１′）［Ａ１′］は、暗号化・復号化部２４において暗号アルゴリズムＡ１に基づいて秘密鍵Ｋｃｉにより暗号化される。

【０１００】

この作成された暗号文Ｅ（Ａ１，Ｋｃｉ）［ＩＤＡ１′｜Ｅ１（Ｋｉ）［ＫＡ１′］｜Ｅ２（ＫＡ１′）［Ａ１′］］と、ＩＤｃと、ＩＤＡ１とがセンター３の通信装置によりネットワーク１を介して端末２ｉに送信される。

【０１０１】

この暗号通信を受信した端末２ｉにおいては、その受信情報が制御部１１に読み込まれ、暗号アルゴリズム格納部１３に対しＩＤＡ１が出力され、鍵情報格納部１２に対しＩＤｃ及びＩＤＡ１が出力される。

【０１０２】

鍵情報格納部１５からは、入力されたＩＤ情報に基づき、鍵情報復号化部１５に対し暗号化された秘密鍵Ｅ１（Ｋｉ）［Ｋｃｉ］及びアルゴリズム復号化鍵Ｅ１（Ｋｉ）［ＫＡ１］が出力される。

【０１０３】

この各暗号化された鍵情報が入力された鍵情報復号化部１２においては、端末固有の鍵情報Ｋｉによってこれらが復号化される。ここで鍵ＫＡ１は暗号アルゴリズム復号化部１６へ秘密鍵Ｋｃｉは暗号化・復号化部１４へそれぞれ出力される。

【０１０４】

一方、制御部１１からＩＤＡ１を入力された暗号アルゴリズム格納部１３からは、暗号アルゴリズム復号化部１６に対し暗号化された暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］が出力される。これを受けた暗号アルゴリズム復号化部１６において、鍵情報復号化部１５から入力されたアルゴリズム復号化鍵ＫＡ１により暗号化された暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］が復号化され、暗号化・復号化部に対しＡ１が出力される。

【０１０５】

暗号化・復号化部１４では、センター３から受け取った暗号文Ｅ（Ａ１，Ｋｃｉ）［ＩＤＡ１′｜Ｅ１（Ｋｉ）［ＫＡ１′］｜Ｅ２（ＫＡ１′）［Ａ１′］］が、暗号アルゴリズムＡ１及び密鍵Ｋｃｉによって復号化される。この復号化が行われた結果、ＩＤＡ１′と対応付けて鍵情報格納部１２にＥ１（Ｋｉ）［ＫＡ１′］が出力され、暗号アルゴリズム復号化部１３にＥ２（ＫＡ１′）［Ａ１′］が出力される。

【０１０６】

こうして、鍵情報格納部１２及び暗号アルゴリズム復号化部１３に対し、暗号アルゴリズムＡ１′のＩＤ情報に対応して、暗号化された鍵情報及び暗号化された暗号アルゴリズムが登録されることになる。したがって、以降、ＩＤＡ１′を受けると、これらの各部１２及び１３はそれぞれＩＤＡ１′についての情報を出力するようになる。

【０１０７】

上述したように、本発明の実施の形態に係る暗号通信端末は、制御部１１にて使用すべき暗号アルゴリズムを指定し、これに対応して暗号アルゴリズム格納部１３，鍵情報格納部１２及び暗号化・復号化部１４を設けたので、複数の暗号アルゴリズムから通信毎にアルゴリズムを選択して暗号通信を行うことができ、解

読される可能性が高くなったアルゴリズムを用いないようにすることで通信の安全性を高めることができる。

【０１０８】

また、本実施形態の暗号通信端末では、暗号アルゴリズム自体を暗号化して暗号アルゴリズム格納部１３に格納しているので、万一暗号アルゴリズムが盗まれた場合でも、そのアルゴリズムの解読や悪用を防止することができる。

【０１０９】

さらに、暗号通信用の鍵やアルゴリズム復号化鍵自体も暗号化がなされているので、これらの鍵が盗まれた場合の悪用を防止することができる。例えば暗号化されたアルゴリズム復号化鍵と暗号化された暗号アルゴリズムとが同時に盗まれても安全性は保持される。

【０１１０】

さらに、本実施形態の暗号通信端末では、新たな暗号アルゴリズム及びアルゴリズム復号化鍵を要求した場合に、その応答を復号し、それぞれを暗号アルゴリズム格納部１３及び鍵情報格納部１３に格納するようにしているので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録することができる。さらに一旦登録されると、次回からはアルゴリズムＩＤを指定するだけでその使用が可能になるため、取得したアルゴリズムを容易に使用可能状態とすることができる。

【０１１１】

また、本実施形態の暗号通信端末では、端末固有の鍵Ｋｉ等の保管あるいは同鍵Ｋｉ等を扱う鍵情報復号化部１５に、ＩＣカード等、内部構造を解析されにくい耐タンパー装置を用いるようにしたので、固有の鍵を不正に取得しようとする行為に対して高い防御力を発揮することができ、ひいては暗号アルゴリズムの不正流出を防ぐことができる。

【０１１２】

また、本実施形態の暗号通信センター装置は、更新用暗号アルゴリズム格納部２６と、鍵情報格納部２２を備え、要求された暗号アルゴリズム及びアルゴリズム復号化鍵を暗号化して要求端末に送信するようにしたので、新規暗号アルゴリ

ズムをネットワークを介して安全かつ効率的に配布することができる。

【０１１３】

したがって、現在使用している暗号方式が破られてしまったような場合でも、すぐに新しい暗号方式を更新することができ、安全なネットワーク通信の継続を容易に実現することができる。

【０１１４】

また、本実施形態の暗号通信センター装置は、各端末２が有する端末固有の鍵によってアルゴリズム復号化鍵を暗号化するようにしたので、万一配布したアルゴリズム復号鍵が盗まれた場合でも、効果的にアルゴリズム復号化鍵の秘匿性を保持することができる。

【０１１５】

なお、暗号通信端末同士からなる暗号通信システム、あるいはこれに暗号通信センター装置を加えた暗号通信システムにおいても、上記と同様な効果を得ることができる。

【０１１６】

（発明の第２の実施の形態）

本実施形態では、第１の実施形態の暗号通信システムにおいて、端末２が保持していない暗号アルゴリズムを取得する他の登録（更新）手順について説明する。

【０１１７】

本実施形態の暗号通信システムは、第１の実施形態における暗号通信システムと同様に構成されている。相違点は、返される暗号アルゴリズム及びアルゴリズム復号化鍵が異なる点である。このために、制御部１１は、第１の実施形態と同様に構成される他、端末２が更新要求する暗号アルゴリズムを選択するようになっている。これらは構成上の相違というよりは、端末２から送信するＩＤ情報及び又はＩＤ情報送信先によって変わる動作上の相違である。なお、本実施形態では第１の実施形態と同一部分には同一符号を付して詳細説明を省略する。

【０１１８】

以下、本実施形態の動作について説明するが、既に登録された暗号アルゴリズ

ムによる暗号通信は第１の実施形態と同様であるので省略し、新たに登録すべきアルゴリズムについて、第１の実施形態で説明した更新手順＃１と異なる更新手順＃２について説明する。

【０１１９】

図６は本発明の第２の実施の形態に係る暗号通信システムにおいて暗号アルゴリズムのみを他の暗号通信端末から取得する更新手順＃２の処理を示す図である。

【０１２０】

ここでは更新手順＃２における第１の手続きとして、まず、暗号アルゴリズムのみを他の暗号通信端末から取得する手続きについて説明する。

【０１２１】

端末２ｊは更新手順＃１若しくは＃２によって暗号アルゴリズムＡ１′を取得している。例えば端末２ｉが自己が保持しない暗号アルゴリズムＡ１′によって端末２ｊと通信しようとするとき、その通信に先立ち、まず、端末２ｉから暗号アルゴリズムＡ１′及びその復号化鍵の取得、登録が行われる。この登録処理は、端末２ｊ及びセンター３のそれぞれに並行して各情報の取得要求がなされることで実現される。

【０１２２】

このために端末２ｉが端末２ｊに対し新しい暗号アルゴリズムＡ１′を要求する場合、まず、端末２ｉからＩＤｉ、更新する暗号アルゴリズムのＩＤ情報ＩＤＡ１′及び更新の際使用する暗号アルゴリズムのＩＤ情報ＩＤＡ１が端末２ｊに対して送信される。

【０１２３】

これらの情報を受け取った端末２ｊにおいては、当該受信情報が制御部１１に読み込まれ、制御部１１から暗号アルゴリズム格納部１３にＩＤＡ１及びＩＤＡ１′が出力される。また、鍵情報格納部１２に対しＩＤｉ及びＩＤＡ１が出力される。

【０１２４】

ＩＤ情報が入力された鍵情報格納部１２からは鍵情報復号化部１５に対し暗号

化された秘密鍵Ｅ１（Ｋｊ）［Ｋｉｊ］及びアルゴリズム復号化鍵Ｅ１（Ｋｊ）［ＫＡｌ］が出力される。さらに、鍵情報復号化部１５では暗号化された鍵情報がパスワードやＩＣカードに保存されている鍵などの端末固有の鍵情報Ｋｊによって復号化され、鍵ＫＡｌが暗号アルゴリズム復号化部へ鍵Ｋｉｊが暗号化・復号化部へそれぞれ出力される。

【０１２５】

一方、ＩＤ情報が入力された暗号アルゴリズム格納部１３からは、暗号アルゴリズム復号化部１６に対し暗号通信用の暗号化された暗号アルゴリズムＥ２（ＫＡｌ）［Ａｌ］が出力される。さらに、暗号化・復号化部１４に対し、端末２ｉに送信すべき暗号化された暗号アルゴリズムＥ２（ＫＡｌ′）［Ａｌ′］が出力される。

【０１２６】

暗号アルゴリズム復号化部１６では、入力された暗号化された暗号アルゴリズムＥ２（ＫＡｌ）［Ａｌ］がアルゴリズム復号化鍵ＫＡｌによって復号化され暗号アルゴリズムＡｌが取り出されて、暗号化・復号化部１４に出力される。

【０１２７】

暗号化・復号化部１４においては、入力された暗号アルゴリズムＡｌ、秘密鍵Ｋｉｊによって更新情報Ｅ２（ＫＡｌ′）［Ａｌ′］が暗号化される。この暗号文Ｅ（Ａｌ，Ｋｉｊ）［ＩＤＡｌ′｜Ｅ２（ＫＡｌ′）［Ａｌ′］とＩＤｊとＩＤＡｌとが通信装置によってネットワーク１を介して端末２ｉに送信される。

【０１２８】

この送信情報は端末２ｉにて受信され、当該受信情報が制御部１１に読み込まれ、暗号アルゴリズム格納部１３に対しＩＤＡｌが出力される。また、制御部１１からは鍵情報格納部１２に対しＩＤｊ及びＩＤＡｌが出力される。

【０１２９】

入力されたＩＤ情報に基づき、鍵情報格納部１２からは鍵情報復号化部１５に対し、暗号化された秘密鍵Ｅ１（Ｋｉ）［Ｋｉｊ］及びアルゴリズム復号化鍵Ｅ１（Ｋｉ）［ＫＡｌ］が出力される。

【０１３０】

この入力された暗号化された鍵情報は、鍵情報復号化部１５においてパスワードやＩＣカードに保存されている鍵などの端末固有の鍵情報Ｋｉによって復号化される。この復号化された鍵のうち、鍵ＫＡｌは暗号アルゴリズム復号化部１６へ出力され、端末間暗号通信用の鍵Ｋｉｊは暗号化・復号化部１４へそれぞれ出力される。

【０１３１】

一方、暗号アルゴリズム格納部１３からは、入力されたＩＤ情報に基づいて暗号化された暗号アルゴリズムＥ２（ＫＡｌ）［Ａｌ］が暗号アルゴリズム復号化部１６に対し出力される。暗号アルゴリズム復号化部１６においては暗号化された暗号アルゴリズムＥ２（ＫＡｌ）［Ａｌ］がアルゴリズム復号化鍵ＫＡｌによって復号化され、その暗号アルゴリズムＡｌが暗号化・復号化部１４に対し出力される。

【０１３２】

暗号化・復号化部１４においては、端末２ｊから入力された暗号文Ｅ（Ａｌ，Ｋｉｊ）［ＩＤＡｌ′｜Ｅ２（ＫＡｌ′）［Ａｌ′］］が、暗号アルゴリズムＡｌ及び秘密鍵Ｋｉｊによって復号化される。この復号化された情報は、暗号化された暗号アルゴリズムＥ２（ＫＡｌ′）［Ａｌ′］であり、同情報はＩＤＡｌ′と対応付けられて暗号アルゴリズム復号化部１３に登録される。

【０１３３】

このようにして、新たな暗号アルゴリズムＡｌ′が端末２ｉに登録されるが、このアルゴリズムを使用可能状態にするためには、当該情報Ｅ２（ＫＡｌ′）［Ａｌ′］を復号化してＡｌ′を取り出すための復号化鍵ＫＡｌ′を取得する必要がある。この復号化鍵ＫＡｌ′は各端末固有の秘密鍵により暗号化されているため、他の端末２ｊから取得することはできない。したがって、鍵の一括管理を行う暗号通信センター装置３に自己の固有の秘密鍵で暗号化したものを発行してもらう必要がある。

【０１３４】

そこで、次に、更新手順＃２における第２の手続きとして、暗号アルゴリズム復号化鍵ＫＡｌ′を暗号通信センター装置３から取得する手続きについて説明す

る。

【０１３５】

図７は暗号アルゴリズム復号化鍵を暗号通信センター装置から取得する更新手順＃２の処理を示す図である。

【０１３６】

まず、端末２ｉからセンター３に対し、端末２ｉのＩＤ情報ＩＤｉ、要求する暗号アルゴリズム復号化鍵のＩＤ情報ＩＤＫＡ１′及びこの暗号通信で使用される暗号アルゴリズムのＩＤ情報ＩＤＡ１が送信される。

【０１３７】

この各ＩＤ情報を受信した暗号通信センター装置３では、まず、受信情報が制御部２１に読み込まれた後、第１実施形態の更新手順＃１と同様にして端末権限管理部２９により権限確認が行われる。なお、権限確認された後に、制御部２１への読み込みが行われてもよい。

【０１３８】

読み込まれた各ＩＤ情報について、制御部２１から暗号アルゴリズム格納部２３に対しＩＤＡ１が出力され、また、鍵情報格納部２２に対しＩＤｉが出力される。また、端末鍵情報格納部２５に対しＩＤｉが出力され、アルゴリズム復号化鍵格納部２６に対しＩＤＫＡ１′が出力される。

【０１３９】

この入力ＩＤ情報に対応し、暗号アルゴリズム格納部２３からは暗号化・復号化部２４に対し暗号アルゴリズムＡ１が出力される。また、鍵情報格納部２２からは入力されたＩＤ情報より、暗号化・復号化部に対し、端末～センター間での暗号通信用の鍵Ｋｃｉが出力される。端末鍵情報格納部２５からは入力されたＩＤ情報より、鍵暗号化部２７に対し端末２ｉ固有の鍵Ｋｉが出力される。さらにアルゴリズム復号化鍵格納部２６からは入力されたＩＤ情報より、鍵暗号化部２７に対し鍵ＫＡ１′が出力される。

【０１４０】

鍵暗号化部２７ではアルゴリズム復号化鍵ＫＡ１′が入力された端末２ｉ固有の鍵Ｋｉにより暗号化され、その暗号化結果であるＥ１（Ｋｉ）［ＫＡ１′］が

暗号化・復号化部２４に出力される。この暗号結果が端末２ｉ専用に作成された暗号化されたアルゴリズム復号化鍵情報である。

【０１４１】

暗号化・復号化部２４では、更新情報Ｅ１（Ｋｉ）［ＫＡ１′］が暗号アルゴリズムＡ１及び秘密鍵Ｋｃｉによって暗号化される。その暗号結果である暗号文Ｅ（Ａ１，Ｋｃｉ）［ＩＤＫＡ１′｜Ｅ１（Ｋｉ）［ＫＡ１′］］とＩＤｃとＩＤＡ１とが通信装置によってネットワーク１を介して端末２ｉに送信される。

【０１４２】

この暗号通信は端末２ｉにて受信され、その受信情報が制御部１１に読み込まれる。制御部１１に読み込まれた情報のうち、ＩＤＡ１が暗号アルゴリズム格納部１３に出力され、また、鍵情報格納部１２に対しＩＤｃ及びＩＤＡ１が出力される。

【０１４３】

ＩＤ情報を入力された鍵情報格納部１２からは鍵情報復号化部１５に対し、ＩＤに対応して暗号化された秘密鍵Ｅ１（Ｋｉ）［Ｋｃｉ］及びアルゴリズム復号化鍵Ｅ１（Ｋｉ）［ＫＡ１］が出力される。これを受けた鍵情報復号化部１５においては、パスワードやＩＣカードに保存されている鍵などの端末固有の鍵情報Ｋｉによって各鍵情報が復号化される。このうち、鍵ＫＡ１が暗号アルゴリズム復号化部１６へ出力され、鍵Ｋｃｉが暗号化・復号化部１４へ出力される。

【０１４４】

一方、暗号アルゴリズム格納部１３からは、入力されたＩＤ情報より、暗号アルゴリズム復号化部１６に対し暗号化された暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］が出力される。

【０１４５】

この暗号化された暗号アルゴリズムＥ２（ＫＡ１）［Ａ１］は、暗号アルゴリズム復号化部１６においてアルゴリズム復号化鍵ＫＡ１により復号化され、その復号結果である暗号アルゴリズムＡ１が暗号化・復号化部１４に出力される。

【０１４６】

暗号化・復号化部１４においては、センター３から受信した暗号文Ｅ（Ａ１，

Ｋｃｉ）［ＩＤＫＡ１′｜Ｅ１（Ｋｉ）［ＫＡ１′］］が、暗号アルゴリズムＡ１及び秘密鍵Ｋｃｉによって復号化される。この復号Ｅ１（Ｋｉ）［ＫＡ１′］は、ＩＤＫＡ１′に対応付けて鍵情報格納部１２に登録される。

【０１４７】

上述したように、本発明の実施の形態に係る暗号通信システムは、第１の実施形態と同様な効果が得られる他、第１の実施形態で説明した更新手順＃１では新しい暗号アルゴリズムと暗号アルゴリズムを復号化するための鍵の両方ともをセンターに要求し、センターは要求された２つを端末２に送っているのに対し、更新手順＃２では、他の端末に新しい暗号アルゴリズム、センター３に対応するアルゴリズム復号化鍵を要求しており、手順＃２のほうがセンター３の負荷を減らすことができる。

【０１４８】

また、更新手順＃２の場合でも、暗号アルゴリズム送信処理及びアルゴリズム復号鍵送信処理が、端末及びセンターで並列して行われるので、手順＃１の場合と同様な時間でこれらを取得することができる。

【０１４９】

なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【０１５０】

例えば各実施形態では、各端末２が保持し、また、センター３が管理する全端末２の固有の鍵Ｋｉ，Ｋｊ等をＤＥＳ等で用いられる共通秘密鍵の場合で説明した。しかし、本発明はこのような場合に限られるものではない。例えばＲＳＡ等の公開鍵方式を用い、各端末２が秘密鍵を保持し、センター３では公開鍵を保持するようにしてもよい。例えばセンター側でのＫｉは公開鍵となり、端末側のＫｉは秘密鍵となる。

【０１５１】

また、各実施形態で説明したセンター３においては、暗号アルゴリズム復号化部１６や鍵情報復号化部１５を備えていないが、これらをセンター３に備え、また、通信に用いる暗号アルゴリズムや鍵も暗号化して格納し、端末２と同一の暗

号通信機能を持たせるようにしてもよい。つまり、センター３側の通信機能はその秘密保持力の強さや外部からのアクセス環境等の種々の状況に応じて適宜な者とすることができる。

【０１５２】

また、実施形態では、ＬＡＮやＷＡＮ、あるいはインターネット等を介して端末２間あるいはセンター３～端末２間で暗号通信する場合で説明したが、本発明の適用範囲はこのような場合に限られるものではない。

【０１５３】

例えばＬＡＮやＷＡＮとして用いる場合であっても、他人同士での通信ばかりでなく、同一企業内の企業内情報管理システムに適用させることができる。企業内といえでも権限無き者に対しては情報を公開すべきでない場合も多いからである。また、メールシステムに本発明を適用させるのも効果的である。

【０１５４】

さらに、実施形態における各端末２をファックス送受信装置とし、ファックス間で暗号通信を行う場合に本発明を適用することができる。電話回線といえども盗聴されることがあるからこれに対応するものである。この場合、容易に暗号方式を変更でき、一旦構築されたファックス網を有効活用できる。さらに、携帯電話やＰＨＳ等を本発明にいう端末２としてもよい。

【０１５５】

また、ケーブルテレビや衛星テレビ、例えばＢＳ放送のスクランブルを暗号と考えたときに、このスクランブルが破られたときに、迅速かつ効果的に新たなスクランブルに変更することができる。このときには、ＢＳチューナが端末２に相当し、また、放送発信側は端末２とセンター３を兼ねることになる。

【０１５６】

同様に、ＩＴビジョンや双方向テレビ等にも適用可能である。このような場合にはセットトップボックスが端末２に相当し、放送側のシステムが端末２とセンター３を兼ねる。

【０１５７】

なお、上記の例でもわかるように、本発明では、端末２間や端末２～センター

３間におけるデータ伝送回線は有線のものに限らず、無線でもよい。

【０１５８】

さらに、本発明でいう端末は、いわゆる計算機装置単体のみにその機能がすべて保持されている場合に限定されるものではない。例えば実施形態で説明した発明を構成する機能が、サーバ計算機やその他の計算機に分散して設けられているような場合でも、単一の計算機装置にこだわらずにこれらの機能を集めたものが本発明でいう端末である。

【０１５９】

なお、実施形態に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【０１６０】

ここで本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【０１６１】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【０１６２】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【０１６３】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【０１６４】

なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【０１６５】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１６６】

【発明の効果】

以上詳記したように本発明によれば、暗号アルゴリズムを選択的して暗号通信を行うことができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することができる。

【０１６７】

また、本発明によれば、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係る暗号通信システムの一例を示す構成図。

【図２】

暗号通信端末の構成例を示すブロック図。

【図３】

暗号通信センター装置の構成例を示すブロック図。

【図４】

端末間で暗号通信が行われる様子を示す図。

【図５】

暗号アルゴリズム及びその復号鍵のすべてを暗号通信センター装置３から取得する更新手順＃１の処理を示す図。

【図６】

本発明の第２の実施の形態に係る暗号通信システムにおいて暗号アルゴリズムのみを他の暗号通信端末から取得する更新手順＃２の処理を示す図。

【図７】

暗号アルゴリズム復号化鍵を暗号通信センター装置から取得する更新手順＃２の処理を示す図。

【符号の説明】

１…ネットワーク

２…暗号通信端末

３…暗号通信センター装置

１１…制御部

１２…鍵情報格納部

１３…暗号アルゴリズム格納部

１４…暗号化・復号化部

１５…鍵情報復号化部

１６…暗号アルゴリズム復号化部

１７…ＩＤ格納部

２１…制御部

２２…鍵情報格納部

２３…暗号アルゴリズム格納部

２４…暗号化・復号化部

２５…端末鍵情報格納部

２６…アルゴリズム復号化鍵格納部

２７…鍵暗号化部

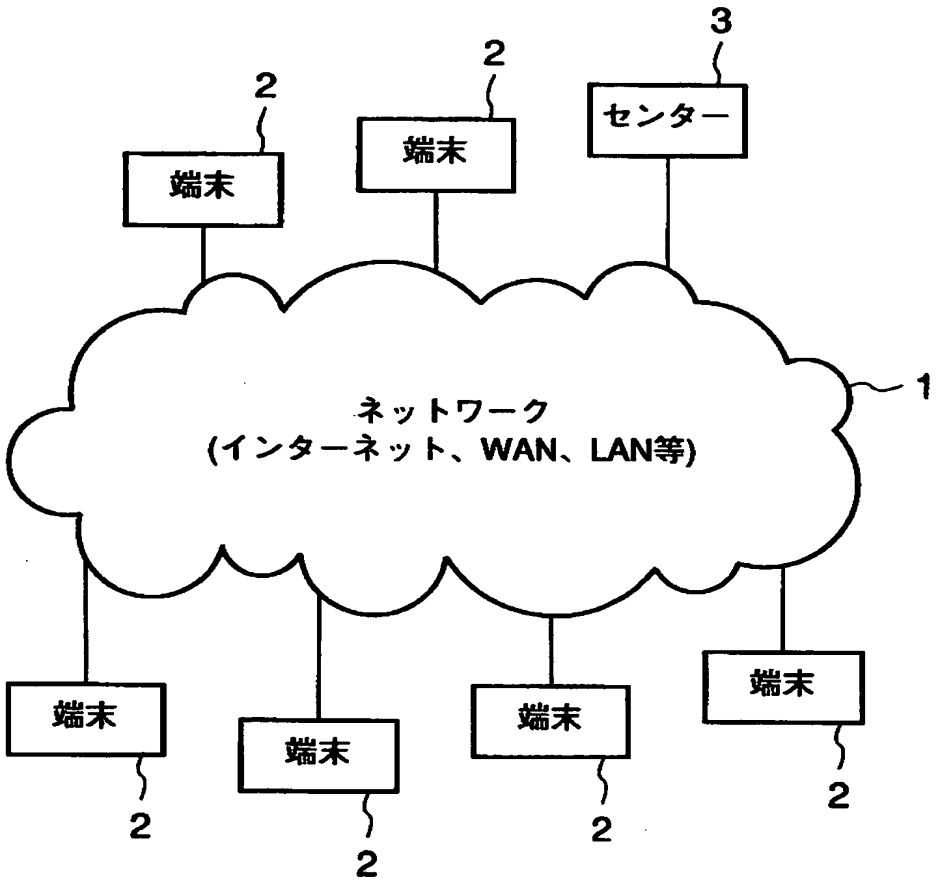
２８…更新用暗号アルゴリズム格納部

２９…端末権限管理部

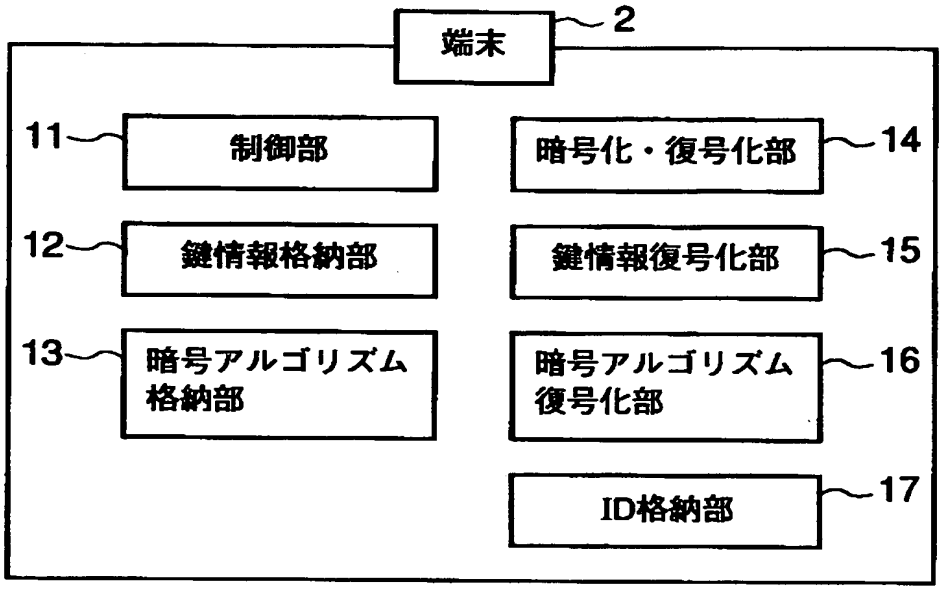
３０…ＩＤ格納部

【書類名】　　図面

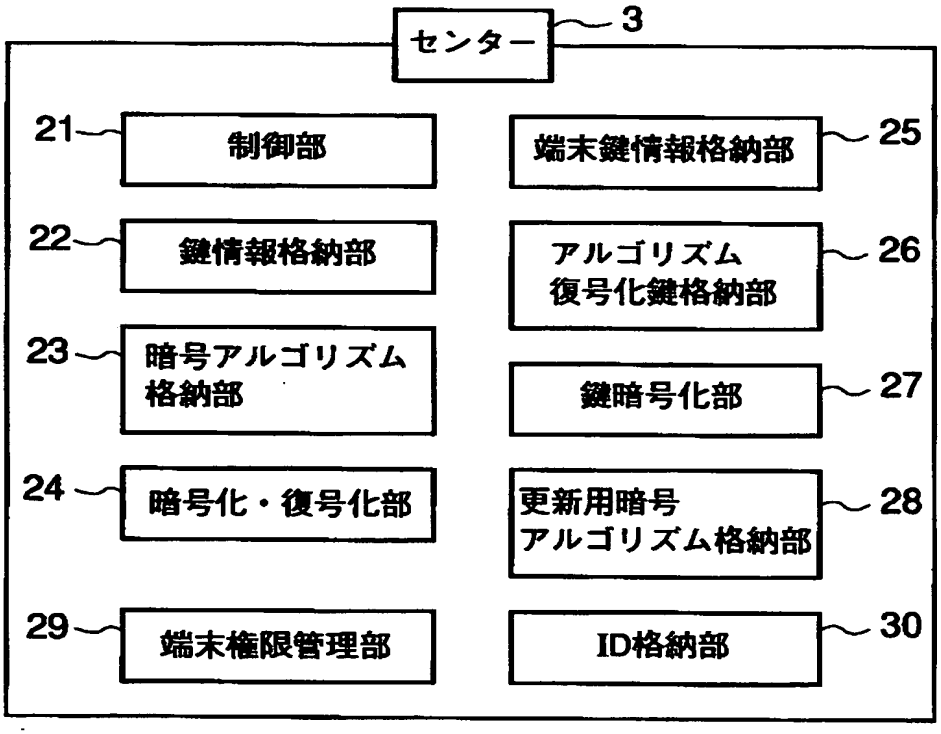
【図１】



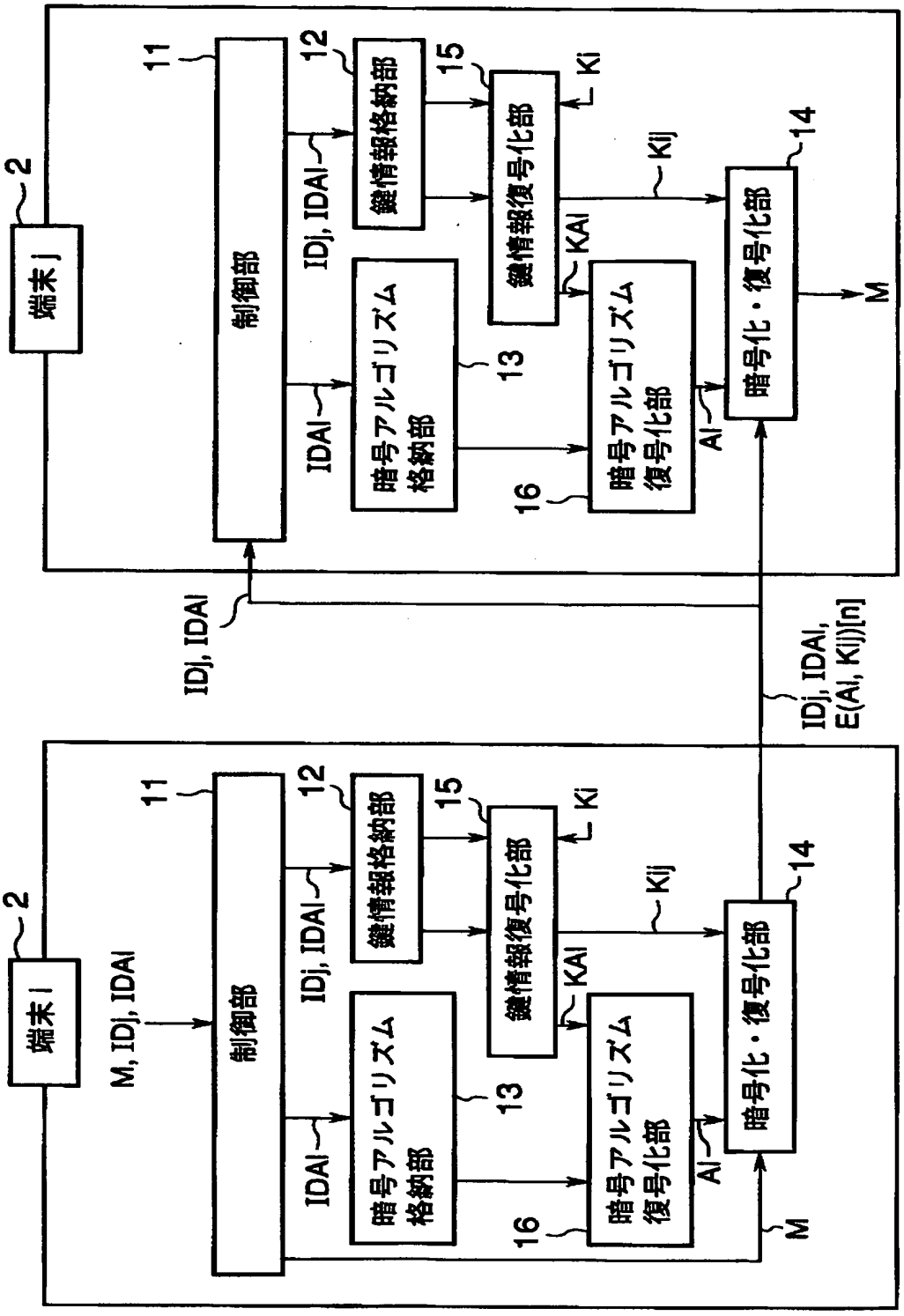
【図２】


端末
2
11
制御部
12
鍵情報格納部
13
暗号アルゴリズム格納部
暗号化・復号化部
14
鍵情報復号化部
15
暗号アルゴリズム復号化部
16
ID格納部
17

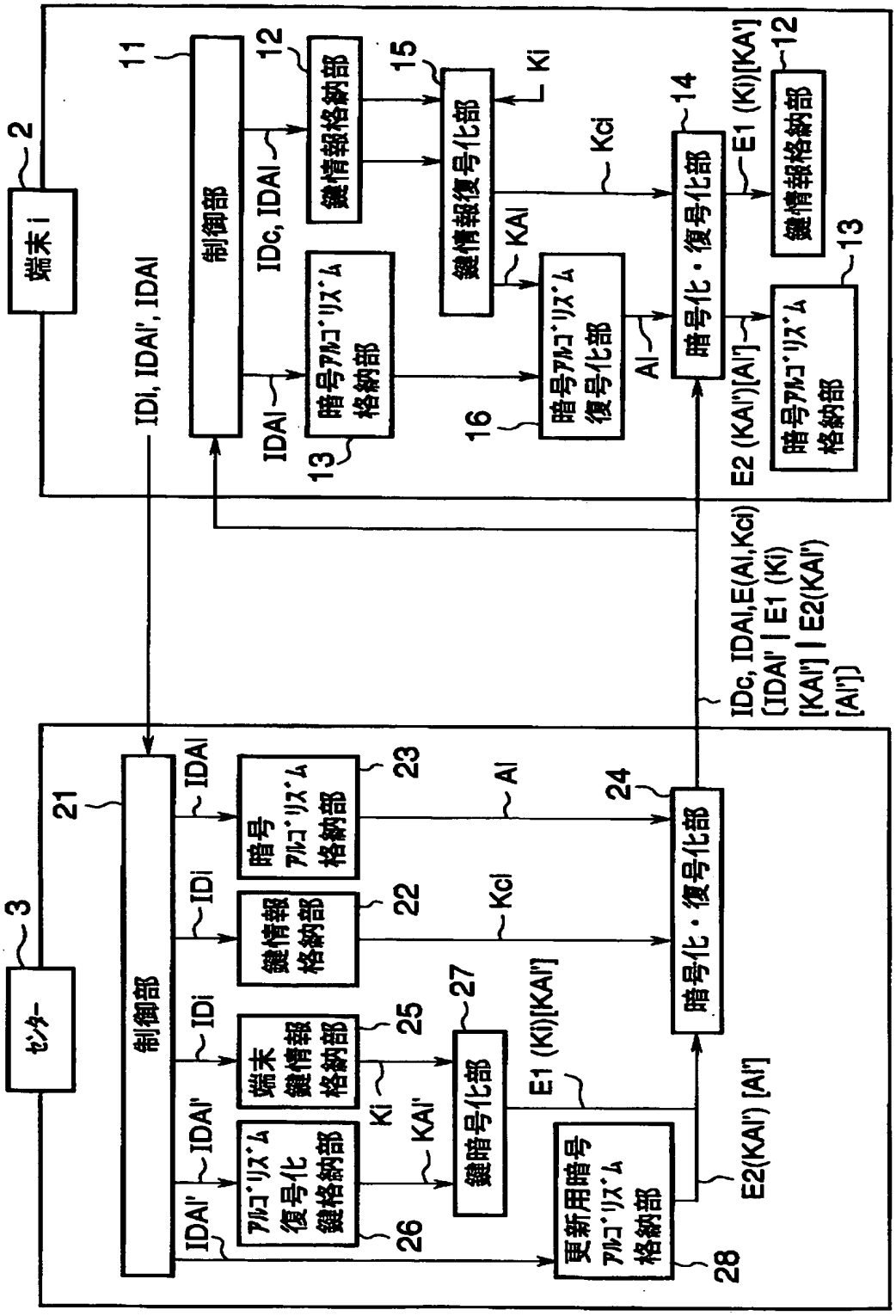
【図３】


センター
3
21
制御部
22
鍵情報格納部
23
暗号アルゴリズム格納部
24
暗号化・復号化部
29
端末権限管理部
端末鍵情報格納部
25
アルゴリズム復号化鍵格納部
26
鍵暗号化部
27
更新用暗号アルゴリズム格納部
28
ID格納部
30

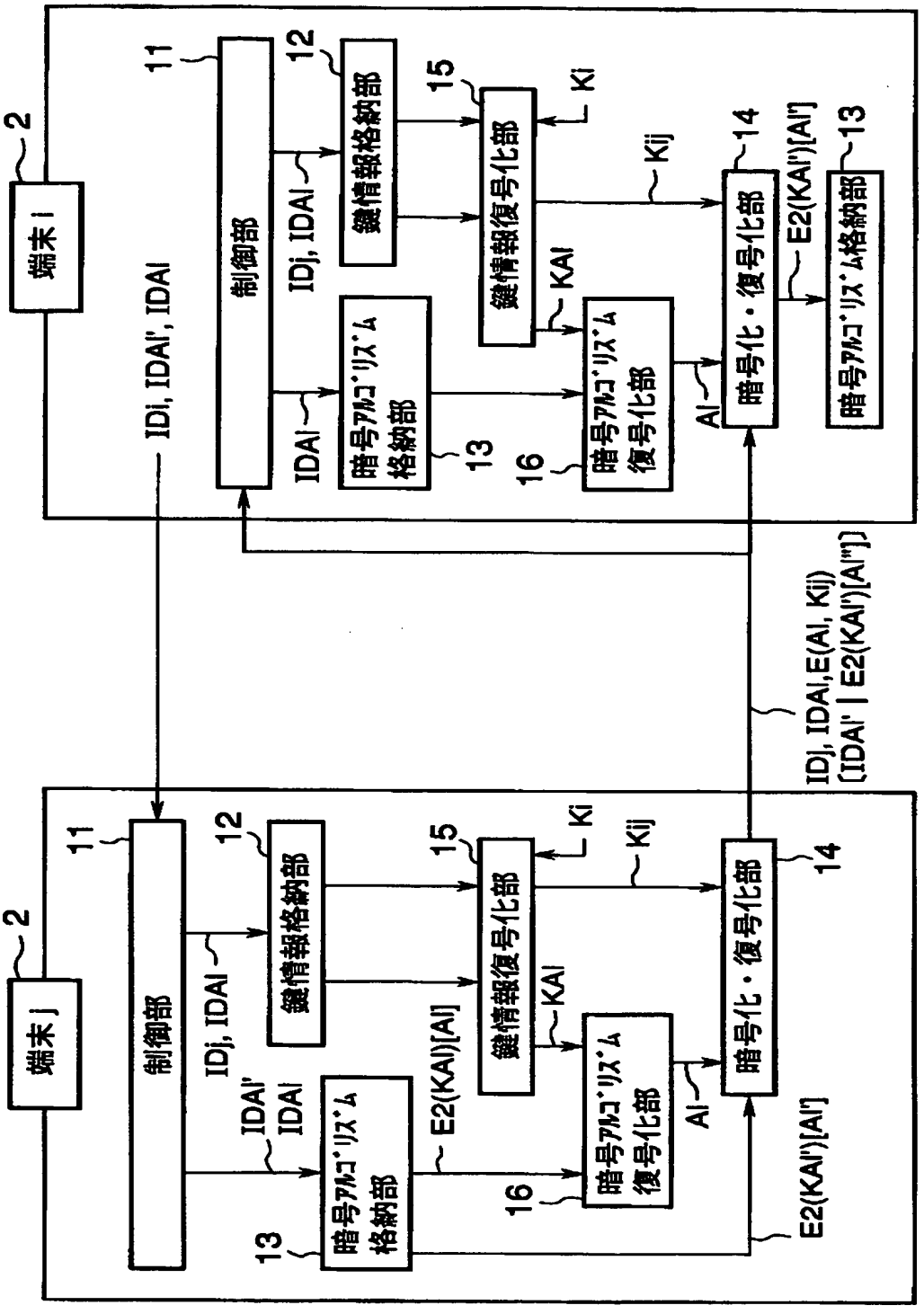
【図４】


端末j
2
制御部
11
鍵情報格納部
12
暗号アルゴリズム格納部
13
鍵情報復号化部
15
暗号アルゴリズム復号化部
16
暗号化・復号化部
14
Ki
Kij
KAI
AI
M
IDj, IDAI
IDAI
IDj, IDAI
IDj, IDAI, E(AI, Kij)[n]
端末i
M, IDj, IDAI
制御部
鍵情報格納部
暗号アルゴリズム格納部
鍵情報復号化部
暗号アルゴリズム復号化部
暗号化・復号化部
Ki
Kij
KAI
AI
M
IDAI
IDj, IDAI

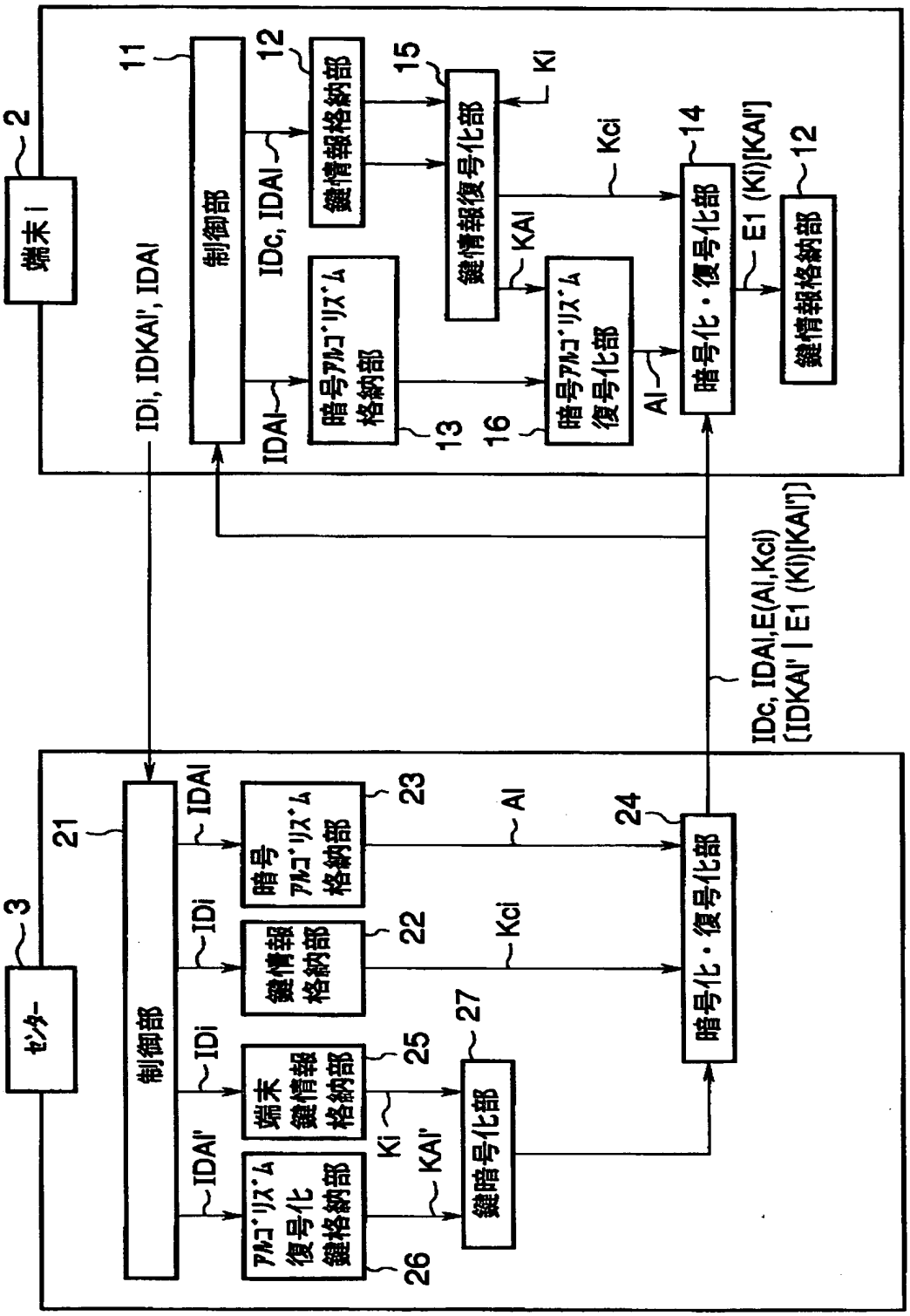
【図５】


端末 i
2
制御部
11
IDi, IDAI', IDAI
IDc, IDAI
12
鍵情報格納部
15
鍵情報復号化部
Ki
Kci
14
暗号化・復号化部
E1 (Ki)[KA']
12
鍵情報格納部
KAI
暗号ｱﾙｺﾞﾘｽﾞﾑ
復号化部
AI
暗号ｱﾙｺﾞﾘｽﾞﾑ
格納部
IDAI
13
16
暗号化・復号化部
E2 (KAI')[AI']
暗号ｱﾙｺﾞﾘｽﾞﾑ
格納部
13
IDc, IDAI,E(AI,Kci)
[IDAI' | E1 (Ki)
[KAI'] | E2(KAI')
[AI']
センター
3
制御部
21
IDAI
暗号
ｱﾙｺﾞﾘｽﾞﾑ
格納部
23
AI
24
暗号化・復号化部
IDi
鍵情報
格納部
22
Kci
IDi
端末
鍵情報
格納部
25
27
鍵暗号化部
E1 (Ki)[KAI']
IDAI'
ｱﾙｺﾞﾘｽﾞﾑ
復号化
鍵格納部
Ki
KAI'
26
IDAI'
更新用暗号
ｱﾙｺﾞﾘｽﾞﾑ
格納部
28
E2(KAI') [AI']

【図６】


端末i
2
11
制御部
12
鍵情報格納部
15
鍵情報復号化部
Ki
Kij
KAI
暗号ｱﾙｺﾞﾘｽﾞﾑ復号化部
AI
14
暗号化・復号化部
E2(KAI')[AI']
暗号ｱﾙｺﾞﾘｽﾞﾑ格納部
13
16
IDi, IDAI', IDAI
IDj, IDAI
IDAI
暗号ｱﾙｺﾞﾘｽﾞﾑ格納部
IDj, IDAI,E(AI, Kij)
〔IDAI' | E2(KAI')[AI'']〕
端末j
2
11
制御部
12
鍵情報格納部
15
鍵情報復号化部
Ki
Kij
KAI
暗号ｱﾙｺﾞﾘｽﾞﾑ復号化部
AI
14
暗号化・復号化部
E2(KAI')[AI']
暗号ｱﾙｺﾞﾘｽﾞﾑ格納部
13
16
IDj, IDAI
IDAI'
IDAI
E2(KAI)[AI]

【図７】


端末i
2
制御部
11
IDi, IDKAI', IDAI
IDAI
IDc, IDAI
12
鍵情報格納部
15
Ki
鍵情報復号化部
Kci
KAI
暗号ｱﾙｺﾞﾘｽﾞﾑ格納部
13
暗号ｱﾙｺﾞﾘｽﾞﾑ復号化部
16
AI
暗号化・復号化部
14
E1 (KI)[KAI']
12
鍵情報格納部
IDc, IDAI,E(AI,Kci)
{IDKAI' | E1 (KI)[KAI']}
センター
3
制御部
21
IDAI
IDi
IDAI'
暗号ｱﾙｺﾞﾘｽﾞﾑ格納部
23
AI
鍵情報格納部
22
Kci
端末鍵情報格納部
25
Ki
27
ｱﾙｺﾞﾘｽﾞﾑ復号化鍵格納部
26
KAI'
鍵暗号化部
暗号化・復号化部
24

【書類名】　　要約書

【要約】

【課題】　暗号アルゴリズムを選択的して暗号通信を行うことができる。

【解決手段】　暗号通信での情報送受信の一方となる暗号通信端末２において、暗号通信に用いる暗号アルゴリズムを１種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部１３と、暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部１２と、暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、暗号アルゴリズム格納部及び鍵情報格納部に対してそれぞれ指定する制御手段１１と、暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段１４とを備えた暗号通信端末。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝